Vista General del Libro Naranja (Orange Book)

Marzo, 2000

Elaborado por:
Departamento de Control de Calidad y Auditoría Informática

Contenido

Vista General del Libro Naranja (Orange Book)

Antes de entrar a fondo con el tema de seguridad, hay que tomar en cuenta que existen diferentes organizaciones, con diferentes tipos de información y por lo tanto con distintos requerimientos de seguridad.

La necesidad de evaluar la seguridad, o de tener una medición confiable, es el motivo principal al desarrollar este documento por el gobierno de los E.E. U.U.

El documento original puede ser consultado en línea en la dirección:

http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

Y obtenerse en las siguientes versiones:
Versión Texto ASCII (txt)
Versión Postscript (ps)
Formato Adobe Portable Document (pdf)
Versión Gzipped Postscript en la dirección:

http://www.radium.ncsc.mil/tpep/library/rainbow/

Introducción

El Libro Naranja es consecuencia de la creciente conciencia de la seguridad por parte el gobierno de los Estados Unidos y de la industria, ambos con la creciente necesidad de estandarizar el propósito y el uso de las computadoras por el gobierno federal.

El Libro Naranja define cuatro extensas divisiones jerárquicas de seguridad para la protección de la información. En orden creciente de confiabilidad se tienen:

D Protección Mínima
C Protección Discrecional
B Protección Obligatoria
A Protección Controlada

Cada división consiste en una o más clases numeradas, entre más grande sea el número se indica un mayor grado de seguridad.

La división C contiene dos distintas clases C1 y C2 (de acuerdo a la nomenclatura adoptada: C2 ofrece una mayor seguridad que C1)
La división B contiene 3 clases B1, B2 y B3 (B3 ofrece mayor seguridad que B2, y B2 ofrece más seguridad que B1).
La división A cuenta con solo una clase A1.

Cada clase se define con un grupo específico de criterios que un sistema debe cubrir, para ser certificado con la evaluación en alguna clase. Este criterio cae en 4 categorías generales: Políticas de seguridad, Responsabilidad, Confianza y Documentación.

Requisitos Fundamentales de la Seguridad en Cómputo

Cualquier discusión sobre seguridad en cómputo necesariamente empieza con una definición de sus requisitos básicos, es decir, realmente qué significa el llamar a un sistema informático "seguro".

En general, un sistema seguro controlará, a través del uso de características específicas de seguridad, el acceso a la información, de forma tal, que solamente los individuos autorizados correctamente, o los procesos que obtienen los permisos adecuados, tendrán acceso para leer, escribir, crear, modificar o eliminar la información.

Se tienen seis requisitos fundamentales, los cuales se derivan de esta declaración básica; cuatro de ellos parten de la necesidad de proporcionar un control de acceso a la información y los dos restantes de cómo puede obtenerse una seguridad demostrable, logrando así un sistema informático confiable.

Políticas de Seguridad.

Requisito 1

Requisito 1 - POLÍTICA DE SEGURIDAD - Debe existir una política de seguridad explícita y bien definida reforzada por el sistema. Identificados los eventos y los objetos, debe haber un conjunto de reglas que son utilizadas por el sistema para determinar si un evento dado se puede permitir para acceder a un objeto específico.

Los sistemas informáticos de interés deben hacer cumplir una política obligatoria de seguridad, en la cual puedan implementarse eficientemente reglas del acceso para manejo de información sensitiva (p.e. clasificaciones) estas reglas deben de incluir requisitos tales como: Ninguna persona que carezca de los permisos apropiados obtendrá el acceso a la información clasificada. Además, los controles de seguridad discrecional se requieren para asegurar que solamente los usuarios o los grupos seleccionados de usuarios puedan obtener el acceso a los datos.(p.e., basarse en una necesidad de conocimientos específicos).

Requisito 2

Requisito 2 - MARCAS - El control de acceso por etiquetas debe de estar asociado a los objetos. Para controlar el acceso a la información almacenada en una computadora, según las reglas de una política obligada de seguridad, debe de ser posible el marcar cada objeto con uno una etiqueta que identifique confiablemente el nivel de la sensibilidad del objeto (p.e., clasificación), y/o los modos de obtener acceso y acordar quien puede tener acceso potencial al objeto.

Responsabilidad

Requisito 3

Requisito 3 - IDENTIFICACIÓN - los eventos individuales deben de ser identificados. Cada acceso a la información debe ser registrado teniendo como base quién está teniendo acceso a la información y qué autorización posee para ocupar cierta clase de información. La información de la identificación y la autorización debe ser administrada con seguridad por el sistema informático y asociar cierta seguridad a cada elemento activo que realice una cierta acción relevante en el sistema.

Requisito 4

Requisito 4 - RESPONSABILIDAD - Las auditorias de la información deben ser selectivamente guardadas y protegidas de las acciones que puedan afectar la seguridad y de testa forma poder rastrear al responsable. Un sistema confiable debe tener la capacidad de registrar la ocurrencia de acontecimientos relevantes sobre seguridad en una bitacora auditable. Además de poseer la capacidad de seleccionar los eventos a auditar para ser registrados, es necesario para reducir al mínimo el costo de la revisión y permitir un análisis eficiente. Este tipo de registros o bitácoras, deben de estar protegidos contra la modificación y la destrucción no autorizada, y deben permitir la detección y la investigación posterior de las violaciones de seguridad.

Confianza

Requisito 5

Requisito 5 - ASEGURAMIENTO - el sistema informático debe contener los mecanismos de hardware/software que puedan ser evaluados independientemente para proporcionar una seguridad suficiente que el sistema haga cumplir los requisitos 1 a 4 mencionados anteriormente. Para asegurar que los requisitos de política de seguridad, marcas, identificación, y responsabilidad de la seguridad son hechos cumplir por un sistema de cómputo, deben ser identificados como una colección unificada de hardware y software que controle y ejecute esas funciones. Estos mecanismos son típicamente incluidos en el sistema operativo y se diseñan para realizar las tareas asignadas de una manera segura. La base para confiar en tales mecanismos del sistema operativo, radica en su configuración operacional, la cual debe ser claramente documentada a fin de hacer posible el examinar independientemente los eventos para su evaluación.

Requisito 6

Requisito 6 - PROTECCIÓN CONTINUA - los mecanismos de seguridad que hacen cumplir estos requisitos básicos, se deben de proteger continuamente contra cambios no autorizados o modificaciones que traten de alterarlos. Ningún sistema de cómputo puede ser considerado verdaderamente seguro si los mecanismos que hacen cumplir las políticas de seguridad, están sujetos a modificaciones no autorizadas. El requisito de protección continua tiene implicaciones directas a través del ciclo de vida de los sistemas.

Cuál es el Propósito del Libro Naranja.

De acuerdo con el texto mismo, el criterio de evaluación se desarrolla con 3 objetivos básicos:

Medición

Para proporcionar de elementos cuantificables al Departamento de Defensa (DoD) con los cuales poder evaluar el grado de confianza que se puede tener en los sistemas informáticos seguros, para el proceso de clasificación de información sensitiva.

El proveer a los usuarios con un criterio con el cual se evalúe la confianza que se puede tener en un sistema de cómputo para el procesamiento de la seguridad o clasificación de información sensitiva. Por ejemplo, un usuario puede confiar que un sistema B2 es más seguro que un sistema C2.

Dirección

Para proporcionar un estándar a los fabricantes en cuanto a las características de seguridad que deben de implementar en sus productos nuevos y planearla con anticipación, para aplicarla en sus productos comerciales y así ofrecer sistemas que satisfacen requisitos de seguridad (con énfasis determinado en la prevención del acceso de datos) para las aplicaciones sensitivas.

Adquisición

Adquisición

El proporcionar las bases para especificar los requerimientos de seguridad en adquisiciones determinadas.

Más que una especificación de requerimientos de seguridad, y tener vendedores que respondan con una gama de piezas. El libro naranja proporciona una vía clara de especificaciones en un juego coordinado de funciones de seguridad. Un cliente puede estar seguro que el sistema que va a adquirir fue realmente verificado para los distintos grados de seguridad.

Las categorías de seguridad del DoD van desde D (Protección Mínima) hasta A (Protección Verificada).

A continuación se presenta un breve resumen las características de cada una de estas categorías y los niveles que tiene cada una.

D- Protección Mínima

Esta división contiene solamente una clase. Esta reservada para los sistemas que han sido evaluados que pero que no pueden cumplir los requisitos para una clase más alta de la evaluación.

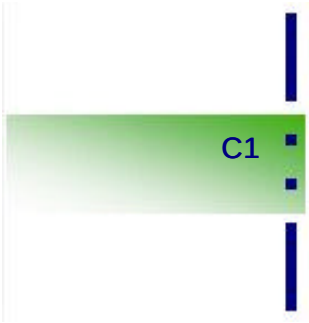
Cualquier sistema que no cumple con cualquier otra categoría, o ha dejado de recibir una clasificación más alta. El sistema DOS para PCs se cae en esta categoría.

C- Protección Discrecional

Las clases en esta división proporcionan una Protección discrecional (necesidad – de - identificación) y, a través de inclusión de capacidades de auditoria, exige la responsabilidad de los usuarios de las acciones que realiza.

La protección discrecional se aplica a una Base de Computadoras Confiables (TCB) con protección de objetos optativos (p.e. archivo, directorio, dispositivos, etc.).

C1- Protección de Seguridad discrecional.

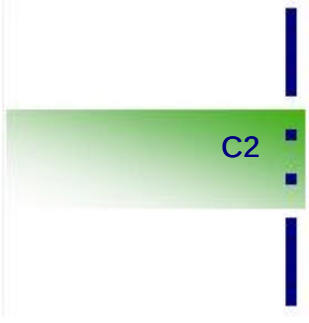


Las TCB de un sistema de la clase C1, deben cubrir los requisitos de seguridad discrecional proporcionando la separación de usuarios y de datos. Incorporar algún mecanismo de control y acreditación, así como la capacidad de hacer cumplir las restricciones de acceso de una base individual, es decir, garantizar de una forma convincente a los usuarios de que sus proyectos o información privada esta protegida y evitar que otros usuarios accidentalmente puedan leer o destruir sus datos. Se supone que en el ambiente de la clase C1 existe cooperación entre los usuarios y además todos ellos procesan datos en el mismo nivel(es) de sensitividad.
Los requisitos mínimos para los sistemas con asignación de la clase C1 son:

- Protección de archivos optativa, por ejemplo Control de Listas de Acceso (ACLs), Protección a Usuario/ Grupo/Público.
- Usualmente para usuarios que están todos en el mismo nivel de seguridad.
- Protección de la contraseña y banco de datos seguro de autorizaciones (ADB).
- Protección del modo de operación del sistema.
- Verificación de Integridad del TCB.
- Documentación de Seguridad del Usuario.
- Documentación de Seguridad del Administración de Sistemas.
- Documentación para Comprobación de la Seguridad.
- Diseño de documentación de TCB.
- Típicamente para usuarios en el mismo nivel de seguridad.

Ejemplo de estos sistemas son las primeras versiones de

C2- Protección de Acceso Controlado.



Los sistemas en esta clase hacen cumplir más fielmente un control de acceso discrecional más fino que los sistemas C1, haciendo responsable individualmente a los usuarios de sus acciones a través de procedimientos de conexión, revisión de eventos relevantes de seguridad, y el aislamiento de recursos.

Los siguientes son requisitos mínimos para los sistemas con asignación de clase (C2):

- La protección de objetos puede estar con base al usuario, ej. De un ACL o una base de datos del administrador.
- La autorización para accesar sólo puede ser asignada por usuarios autorizados.
- Protección de reuso de objetos (p.e. para evitar reasignación de permisos de seguridad de objetos borrados).
- Identificación obligatoria y procedimientos de autorización para los usuarios, p.e. contraseñas.
- Auditoria de eventos de seguridad.
- Protección del modo de operación del sistema.
- Agrega protección para autorizaciones y auditoría de datos.
- Documentación de la información como C1 plus al examinar la auditoría de la información.

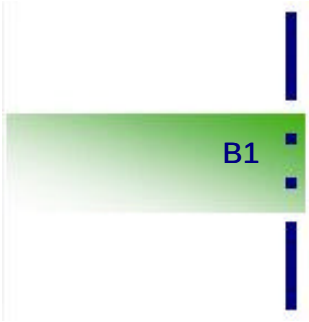
Algunos sistemas típicos son versiones posteriores de Unix, VMS.

B- Protección Obligatoria

La división B especifica que el sistema de protección del TCB debe ser obligatorio, no solo discrecional.

La noción de un TCB que preserve la integridad de etiquetas de sensibilidad de la información y se utilizan para hacer cumplir un conjunto de reglas obligatorias del control de acceso, es un requisito importante en esta división. Los sistemas en esta división deben llevar las etiquetas de sensibilidad en las estructuras de datos importantes del sistema. El desarrollador del sistema también debe proporcionar un modelo de política de seguridad en el cual se basa el TCB y equipar por medio de una serie de especificaciones al TCB. Evidentemente debe ser proporcionada una demostración que sirva para aclarar el concepto del monitor de referencia y su forma de implementarlo.

B1- Protección de Seguridad por Etiquetas

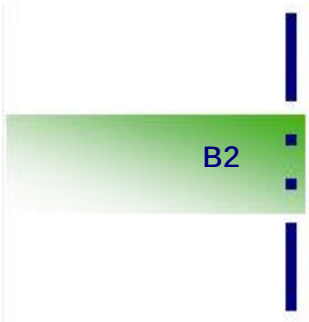


Los sistemas de la clase B1 requieren todas las características solicitadas para la clase C2. Además una declaración informal del modelo de la política de seguridad, de las etiquetas de los datos, y del control de acceso obligatorio sobre los eventos y objetos nombrados debe estar presente. Debe existir la capacidad para etiquetar exactamente la información exportada. Cualquier defecto identificado al hacer las pruebas debe ser eliminado.

Los siguientes son los requisitos mínimos para los sistemas con asignaron de grado de la clase B1:

- Seguridad obligatoria y acceso por etiquetas a todos los objetos, ej. archivos, procesos, dispositivos, etc.
- Verificación de la Integridad de las etiquetas.
- Auditoria de objetos Etiquetados.
- Control de acceso obligatorio.
- Habilidad de especificar el nivel de seguridad impreso en salidas legibles al humano (ej. impresiones.).

B2- Protección Estructurada

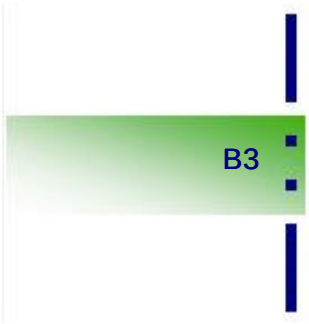


En los sistemas de clase B2, los TCB deben estar basados en una documentación formal clara y contar con un modelo de política de seguridad bien definido que requiera un control de acceso discrecional y obligatorio, las imposiciones a los sistemas encontradas en la clase B1, se deben extender a todos los eventos y objetos en sistemas ADP. Además, los canales secretos son direccionados. El TCB se debe estar cuidadosamente estructurado en elementos de protección críticos y elementos de protección no críticos. La interfaz de TCB deberá estar bien definida así como el diseño y la activación de la implementación del TCB le permiten ser sujeto de prueba y revisión más completa. Se consolidan los mecanismos de autentificación, el manejo de recursos seguros se proporciona en forma de ayuda para las funciones del administrador y del operador del sistema, y se imponen controles rigurosos de la administración de configuración. El sistema es relativamente resistente a la penetración.
Los siguientes son requisitos mínimos para los sistemas con asignación de grado de la clase B2:

- Notificación de cambios del nivel de seguridad que afecten interactivamente a los usuarios.
- Etiquetas de dispositivos jerárquicas.
- Acceso obligatorio sobre todos los objetos y dispositivos.
- Rutas Confiables de comunicaciones entre usuario y sistema.
- Rastreo de los canales secretos de almacenamiento.
- Modo de operación del sistema más firme en multinivel en unidades independientes.
- Análisis de canales seguros.
- Comprobación de la seguridad mejorada.
- Modelos formales de TCB.
- Versión, actualización y análisis de parches y auditoria.

Un ejemplo de estos sistemas operativos es el Honeywell Multics.

B3- Protección por Dominios



En la clase B3 los TCB debe satisfacer los requisitos de herramientas de monitoreo como un "monitor de referencia" que Interviene en todos los accesos de usuarios a los objetos, a fin de ser comprobada, y que sea lo bastante pequeña para ser sujeta al análisis y pruebas. Al final, el TCB debe estar estructurado para excluir el código no esencial para aplicar la política de seguridad, mediante ingeniería de sistemas durante el diseño y la implementación del TCB, orientada hacia la reducción de su complejidad al mínimo.

Debe de contar también con un Administrador de Seguridad, los mecanismos de auditoria se amplían para señalar acontecimientos relevantes de la seguridad, y se necesitan procedimientos de recuperación del sistema. El sistema es altamente resistente a la penetración.
Los siguientes son requisitos mínimos para los sistemas con asignación de un grado de clase B3:

- ACL's adicionales basado en grupos e identificadores.
- Rutas de acceso confiables y autentificación.
- Análisis automático de la seguridad.
- Modelos más formales de TCB.
- Auditoría de eventos de seguridad.
- Recuperación confiable después de baja del sistema y documentación relevante.
- Cero defectos del diseño del TCB, y mínima ejecución de errores.

Protección Verificada

Esta división se caracteriza por el uso de métodos formales para la verificación de seguridad y así garantizar que los controles de seguridad obligatoria y discrecional empleados en el sistema pueden proteger con eficacia la información clasificada o sensitiva almacenada o procesada por el sistema. Se requiere de amplia documentación para demostrar que el TCB resuelve los requisitos de seguridad en todos los aspectos del diseño, desarrollo e implementación.

Se deben de cubrir todos los requisitos de B3 más otros criterios adicionales:

A1- Diseño verificado

Los sistemas en la clase (A1) son funcionalmente equivalentes a los de la clase B3 en que no se agrega ningunas características o requisitos arquitectónicos adicionales de la política de seguridad. La característica que distingue los sistemas en esta clase es el análisis derivado de técnicas formales de especificación y la verificación del diseño, y el alto grado de confiabilidad que resulta de la correcta implementación del TCB. Este garantia se desarrolla naturalmente, comenzando con un modelo formal de la política de la seguridad y una especificación formal de alto nivel (FTLS Especificación Normal de Alto Nivel) del diseño. Independiente del lenguaje determinado de la especificación o sistema de la verificación usado, hay cinco criterios importantes para la verificación del diseño de la clase (A1).

- Un modelo formal de la política de seguridad debe ser claramente identificado y documentar, incluyendo una prueba matemática que el modelo es constante con sus axiomas y es suficiente para soportar la política de la seguridad.

- Un FTLS debe ser proporcionado que incluya las definiciones abstractas de las funciones que el TCB se realiza y de los mecanismos de la dotación física y/o de los firmwares que se utilizan para utilizar dominios separados de la ejecución.

- Se debe demostrar que el FTLS del TCB es constante y consistente con el modelo por técnicas formales en lo posible (es decir, donde existen las herramientas de verificación) y las informales de otra manera.

- La implementación del TCB (p.e., en Hardware, firmware, y software) debe mostrar informalmente que es consistente con el FTLS. Los elementos del FTLS deben ser mostrados, usando técnicas informales, que correspondan a los elementos del TCB. El FTLS debe expresar un mecanismo unificado de protección, necesario para satisfacer la política de seguridad, y todos los elementos de este mecanismo de protección deben estar asociados a los elementos del TCB.
- Deben de utilizarse técnicas de análisis formal para identificar y analizar los canales secretos. Las técnicas informales se pueden utilizar para identificar los canales secretos de sincronización. La continua existencia de canales secretos identificados en el sistema debe ser justificada.

A2 en adelante

La Propuesta hecha para los más altos niveles de seguridad se denomina como A2, aunque sus requerimientos aun no han sido definidos formalmente.

Evaluación de Clases y Ejemplo de Sistemas

En la siguiente tabla se resumen los niveles de seguridad establecidos por el Libro naranja, las clases que los integran, el nombre que recibe cada una de estas clases así como ejemplo de algunos de los sistemas han logrado ese grado.

Nivel	Clase	Nombre	Ejemplo
D		Protección Mínima	
	D		Sistemas operativos básicos: MS-DOS
C		Protección Discrecional	
	C1	Protección de Seguridad discrecional	IBM MVS/RACF Cualquier versión de UNIX ordinaria, que no ha sido enviada a una evaluación formal
	C2	Protección de Acceso Controlado	Computer Associates International: ACF/2/MVS Digital Equipment Corporation: VAX/VMS 4.3 HP MPE V/E
B		Protección Obligatoria	
	B1	Protección de seguridad por etiquetas	AT&T System V/MLS UNISIS OS 1100 SecuryWare: CMW+ IBM MVS/ESA
	B2	Protección Estructurada	Honeywell Information System: Multics Trusted Information System XENIX
	B3	Protección por Dominios	Honeywell Federal System XTS-200
A		Protección Verificada	
	A1	Diseño verificado	Honeywell Information System SCOMP Boeing Aerospace : SNS

La figura siguiente compara las clases de evaluación del libro naranja, mostrando las características requeridas para cada clase y en términos generales, como se incrementan los requerimientos de clase a clase. Adicionalmente se presentan cuadros comparativos de cada criterio a evaluar y los cambios más importantes que se necesitan para pasar de un nivel de seguridad u otro.

	C1	C2	B1	B2	B3	A1
Políticas de seguridad						
Control de acceso discrecional						
Reutilización de Objetos						
Etiquetas						
Integridad de Etiquetas						
Exportación de información etiquetada						
Exportación de Dispositivos multinivel.						
Exportación de Dispositivos de nivel único						
Etiquetado de salidas legibles a la persona						
Etiquetas sensitivas de eventos						
Dispositivos etiquetados						
Control de acceso obligatorio						
Responsabilidad						
Identificación y autentificación						
Rutas seguras						
Auditoria						
Confianza						
Arquitectura del sistema						
Integridad del sistema						
Pruebas de seguridad						
Diseño de especificaciones y verificación						
Análisis de canales secretos						
Facilidad de administración de la seguridad						
Administración de configuración						
Recuperación confiable						
Distribución confiable						
Documentación						
Guía del usuario sobre características de seguridad						
Facilidades del manual de seguridad						
Pruebas de documentación						
Diseño de documentación						
	C1	C2	B1	B2	B3	A1

Significado de los claves

	No requerido para esta clase.
	Requerimiento nuevo o mejorado para esta clase
	No se tienen requerimientos adicionales para esta clase

Control de Acceso Discrecional

El Control de Acceso Discrecional (DAC) es un método de restringir el acceso a los archivos (y a otros objetos del sistema) basándose en la identidad de los usuarios y/o los grupos a los que pertenecen. EL DAC es el más común de los mecanismos de control de acceso que se encuentra en los sistemas

C1	C2	B1	B2	B3	A1
Control de acceso discrecional					
La TCB deberá definirse y controlar el acceso entre usuarios registrados y objetos registrados (por ejemplo, archivos y programas). En el sistema ADP El mecanismo de ejecución (por ejemplo controles de usuario / grupo / publico, control de listas de acceso) deberá permitirse a los usuarios el especificar y controlar el compartir ciertos objetos a individuos registrados o grupos definidos o ambos.	**Requerimientos adicionales** Definición de grupos más específicamente El mecanismo de ejecución debe proporcionar controles para limitar la propagación de permisos de acceso El mecanismo de control de acceso discrecional deberá Permitir ya sea una acción de un usuario explícito o un default, proporciona que los objetos sean protegidos de accesos no autorizados. Este control de acceso debe ser capaz de incluir o excluir el acceso de usuarios. El permiso de acceso de un objeto para usuarios que ya no poseen el permiso de acceso deberá ser asignado sólo por los usuarios autorizados	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales	**Requerimientos adicionales** El mecanismo de ejecución debe de ser accesado mediante listas de control El control de acceso debe ser capaz de especificar a cada objeto registrado, una lista de nombres de personas con sus respectivos modos de acceso a ese objeto. Además, para cada uno de los objetos registrados, de ser posible especificar una lista de los individuos registrados y una lista de los grupos o personas registradas con acceso denegado del grupo,	No se tienen requerimientos adicionales

Reutilización de Objetos

La reutilización de Objetos requiere la protección de archivos, memoria y otros objetos en un sistema auditado de ser accesadas accidentalmente por usuarios que no tienen acceso autorizado a ellos. Las características de control de acceso de u sistema ordinario determina quien puede y quien no puede accesar archivos, dispositivos y otros objetos que han sido asignados a usuarios específicos La reasignación de objetos requiere las direcciones que aparecen en esos objetos sean reasignadas.

C1	C2	B1	B2	B3	A1
Reutilización de objetos					
No se requiere	Todas las autorizaciones para la información contenida con un almacenamiento de objetos deberán ser revocadas previamente o con una asignación inicial, asignación o reasignación del tema desde el pool del TCB de los objetos no utilizados y almacenados. La información, incluyendo la representación encriptada de la información, producida por las aciones de un evento previo debe de estar disponible para cualquier evento que obtenga el acceso de un objeto que ha sido ya regresado al sistema	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales

Etiquetas

Las etiquetas y el control de acceso obligatorio son requerimientos separados de la política de seguridad, pero ambas funcionan juntas. Al iniciar en el nivel B1, el libro naranja propone que cada sujeto (p.e. usuario, proceso) y un objeto almacenado (p.e. archivos, directorios, ventanas, socket) tengan una etiqueta sensitiva asociada a él. Una etiqueta sensitiva de usuario especifica el grado, o nivel de confianza, asociado con ese usuario, las etiquetas de usuario sensitivas es usualmente llamada como certificado de paso ó "clearance". Una etiqueta sensitiva de archivo especifica el nivel de confianza que un usuario puede ser capaz de tener al accesar ese archivo.

C1	C2	B1	B2	B3	A1
Etiquetas					
No se requiere	No se requiere	Etiquetas sensitivas asociadas con cada evento y objeto almacenado bajo su control (p.e. procesos, archivos, segmentos, dispositivos) deben ser mantenidos por el TCB. Estas etiquetas deberán ser utilizadas como las bases para las decisiones del control del acceso obligatorio. En orden de importancia de datos no etiquetados, el TCB debe solicitar y recibir de un usuario autorizado el nivel de seguridad de esos datos, y todas las acciones deberán ser auditadas por el TCB	**Requerimientos adicionales** Las etiquetas sensitivas asociadas con cada recurso del sistema ADP (p.e. eventos, objetos almacenados, ROM) que son directamente o indirectamente accesados por eventos externos a él TCB debe ser mantenido por el TCB	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales

Integridad de Etiquetas

La integridad de etiquetas asegura que las etiquetas sensitivas asociadas con eventos y objetos tienen una representación exacta de los niveles de seguridad de estos eventos y objetos
Así una etiqueta sensitiva como TOP SECRET [VENUS] deberá estar asociado con un archivo TOP SECRET que contiene información acerca del planeta Venus

C1	C2	B1	B2	B3	A1
Integridad de etiquetas					
No se requiere	No se requiere	Las Etiquetas sensitivas deberán representar con precisión los niveles de los eventos específicos u objetos con los que estos están asociados Cuando son exportados por el TCB, las etiquetas sensitivas deberán precisar y representar sin ambigüedad las etiquetas internas y deberán estar asociadas con la información que esta siendo exportada.	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales

Exportación de Información Etiquetada

Un sistema confiable debe de asegurar que la información es escrita por el sistema, que la información cuenta con mecanismos de protección asociados a ella. Dos formas de exportar información son asignar un nivel de seguridad a los dispositivos de salida ó escribir etiquetas sensitivas en los datos. Los sistemas valorados como B1 en adelante deben de proporcionar facilidades de exportación segura

Se definen dos tipos de dispositivos para exportar; multinivel y de nivel simple. Cada dispositivo de entrada / salida y canal de comunicaciones en un sistema debe de ser designado de uno o de otro tipo. Cualquier cambio a estas designaciones de dispositivos debe de ser capaz de ser auditado. Típicamente un administrador de sistemas designa dispositivos durante la instalación del sistema o durante su configuración

C1	C2	B1	B2	B3	A1
Exportación de información etiquetada					
No se requiere	No se requiere	El TCB deberá designar cada canal de comunicaciones y dispositivo de entrada / salida, ya sea como de un nivel sencillo o de multinivel. Cualquier cambio en esta designación deberá ser hecha manualmente y deberá ser auditable por el TCB. El TCB deberá mantener y ser capaz de auditar cualquier cambio en los niveles de seguridad o niveles asociados con un canal de comunicaciones o dispositivo de entrada / salida	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales

Dispositivo Multinivel

Un dispositivo multinivel o un canal de comunicaciones multinivel es uno con la capacidad de escribir información con un número diferente de niveles de seguridad. El sistema debe soportar una variedad de especificaciones de niveles de seguridad, desde la más baja (SIN CLASIFICACIÓN) hasta la más alta (ALTAMENTE SECRETA), permitiendo que un dato sea escrito en un dispositivo
Cuando se escribe información en un dispositivo multinivel, se requiere que el sistema tenga alguna forma de asociar un nivel de seguridad a él. Los mecanismos pueden diferir para los diferentes sistemas y los diferentes tipos de dispositivos. Los archivos escritos a este dispositivos pueden tener etiquetas sensitivas agregadas a ellas (usualmente escritas en los encabezados del registro precediendo los datos del archivo). Todo esto para prevenir que un usuario desvíe los controles del sistema con una simple copia de un archivo sensitivo a otro de un sistema inseguro o dispositivo.

C1	C2	B1	B2	B3	A1
Exportación en dispositivos múltinivel					
No se requiere	No se requiere	Cuando el TCB exporta un objeto que es multinivel o un dispositivo de entrada / salida, la etiqueta sensitiva asociada con ese objeto también deberá ser exportada y permanecer residente en el mismo medio físico que la información exportada y deberá estar en la misma forma (p.e. de forma legible a la máquina o en forma legible a la persona). Cuando el TCB exporta o importa un objeto sobre un canal de comunicación multinivel, el protocolo usado en ese canal deberá proporcionar una paridad que evite ambigüedad entre las etiquetas sensitivas y la información asociada que se esta enviando o recibiendo	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales

Dispositivo de Nivel Unico

Un dispositivo de nivel único o un canal de comunicaciones de nivel único es uno capaz de escribir información con sólo un nivel particular de seguridad. Usualmente las terminales, impresoras, dispositivos de cinta y puertos de comunicación están en la categoría de dispositivos de nivel único. El nivel que se especifica para un dispositivo depende usualmente de su localización física o de la seguridad inherente del tipo de dispositivo. Por ejemplo, la instalación de una red contempla varias impresoras en un número determinado de computadoras y oficinas. El administrador debe designar que esas impresoras tengan niveles sensitivos que correspondan al personal que tiene acceso a dichas impresoras.

C1	C2	B1	B2	B3	A1
Exportación en dispositivos de nivel único					
No se requiere	No se requiere	Los dispositivos de niel único de canales de comunicaciones de entrada / salida no son requeridas para mantener las etiquetas sensibles de la información que procesan De cualquier modo, el TCB debe incluir un mecanismo para que el TCB y un usuario autorizado fiable comunique y designe el nivel único de seguridad de la información importada o exportada vía canal de comunicaciones de nivel sencillo o dispositivo de entrada / salida.	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales

Etiquetado de Salidas Legibles a la Persona

El libro naranja es muy claro en cuanto a los requerimientos de cómo deben de hacerse las etiquetas para las salidas legibles al humano (salidas que las personas pueden ver). Estas incluyen páginas de salida impresa, mapas, gráficas y otros indicadores. El administrador del sistema debe de especificar la forma en que las etiquetas van a aparecer en la salida.
Por lo regular se requieren dos tipos de etiquetas: primero, cada salida distinta debe ser etiquetada, al principio y al final, con etiquetas que representen una sensitividad general de la salida. Sí se está imprimiendo el contenido de un archivo Y típicamente se puede ver una página de un banner antes y después del contenido del documento, mostrando claramente la etiqueta sensitiva del archivo. Segundo, cada página de salida impresa debe ser etiquetada, e la parte superior y en la parte inferior, con etiquetas que presenten ya sea una u otra, una sensitividad general de la salida o la sensitividad específica de la información en esa página.

C1	C2	B1	B2	B3	A1
Etiquetas de salida legibles al humano					
No se requiere	No se requiere	El administrador del sistema ADP debe ser capaz de especificar los nombres de las etiquetas imprimibles asociados con las etiquetas sensitivas exportables El TCB debe marcar el inicio y el fin de todas las etiquetas sensitivas legibles a la persona que representen sensitivamente la salida. El TCB deberá, por omisión marcar el límite inferior y superior de cada página legible al hombre, compaginada, de la salida impresa (p.e. Salidas de la impresora) con una etiqueta sensitiva legible al hombre que represente apropiadamente la sensitividad global de la salida o que represente apropiadamente la sensitividad de la información de cada página. Cualquier anulación de estas marcas por defecto deben ser auditables por el TCB	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales

Etiquetas Sensitivas de Eventos

Las etiquetas sensitivas de eventos requieren estados que el sistema pueda notificar a determinado usuario de algún cambio en el nivel de seguridad asociado con un usuario durante una sesión interactiva. Este requerimiento se aplica de los sistemas evaluados B2 en adelante.
La idea de las etiquetas sensitivas a eventos es que el usuario siempre conozca el nivel de seguridad en el que esta trabajando. Los sistemas confiables típicamente despliegan el "clearance" cuando se establece sesión y lo despliegan nuevamente si el nivel de seguridad tiene algún cambio, o automáticamente a petición del usuario.

C1	C2	B1	B2	B3	A1
Etiquetas sensitivas de eventos					
No se requiere	No se requiere	No se requiere	El TCB debe notificar inmediatamente a la terminal del usuario de cada cambio en el nivel de seguridad asociado con ese usuario durante una sesión interactiva. La terminal de usuario debe de ser capaz de buscar el TCB cuando lo desee para desplegar en un evento con etiqueta sensitiva.	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales

Dispositivos Etiquetados

Los dispositivos etiquetados requieren estados que cada dispositivo físico tenga adicionados en el sistema que definan niveles mínimos y máximos de seguridad asociados a ellos, y todos estos son usados para "reforzar las restricciones impuestas por el medio ambiente físico en el cual el dispositivo esta localizado".
Para un dispositivo multinivel, se debe de especificar el nivel mínimo de la información que puede ser enviada a este dispositivo (el mínimo para el dispositivo) y el nivel más alto de información que puede ser enviada al dispositivo (el máximo del dispositivo). Para un dispositivo de un nivel único, el nivel mínimo es el mismo que el nivel máximo

C1	C2	B1	B2	B3	A1
Dispositivos Etiquetados					
No se requiere	No se requiere	No se requiere	El TCB debe soportar la asignación de un nivel mínimo y máximo para todo dispositivo físico adjunto. Estos niveles de seguridad deben de ser usados por el TCB para reforzar las condiciones impuestas por el medio ambiente físico en cada uno de los dispositivos físicos localizados	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales

Control de Acceso Obligatorio

El control de acceso obligatorio es el último requerimiento de la política de seguridad, diferente del control de acceso discrecional, que autoriza a los usuarios específicamente, con sus propias preferencias, quien puede y quién no puede accesar sus archivos, el control de acceso obligatorio pone el control de todos los accesos como decisiones bajo el control del sistema

C1	C2	B1	B2	B3	A1
Control de acceso obligatorio					
No se requiere	No se requiere	El TCB debe reforzar las políticas del control de acceso obligatorio de todos los sujetos y objetos almacenados (procesos, archivos, dispositivos, etc.) A estos sujetos y objetos debe ser asignado una etiqueta sensitiva que sean una combinación e clasificación por nivel jerárquico y categorías no jerárquicas, y las etiquetas deberán ser usadas como la base de las decisiones para el control de acceso obligatorio El TCB debe ser capaz de soportar dos o más niveles de seguridad, los siguientes requerimientos deberán mantenerse para todos los accesos entre sujetos y objetos controlados por el TCB.	Requerimientos adicionales El TCB debe reforzar las políticas del control de acceso obligatorio para todos los recursos(usuarios, objetos almacenados, dispositivos de entrada / salida) que sean accesibles directa o indirectamente por usuarios externos al TCB. Los requerimientos deberán mantenerse para todos los accesos entre todos los usuarios externos a él TCB y todos los objetos accesibles directa o indirectamente por estos usuarios.	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales

C1	C2	B1	B2	B3	A1
		Un sujeto puede leer un objeto solamente si la clasificación jerárquica del nivel de seguridad del sujeto es menor o igual que la clasificación jerárquica de los niveles de seguridad del objeto y la categoría no jerárquica de los niveles de seguridad que se incluyen en todas las categorías no jerárquicas del nivel de seguridad del objeto. Un usuario puede escribir en un objeto solamente si la clasificación jerárquica del nivel de seguridad del sujeto es mayor o igual que la clasificación jerárquica de los niveles de seguridad del objeto y cumple con todas las categorías no jerárquicas de los niveles de seguridad que se incluyen en todas las categorías no jerárquicas del nivel de seguridad del objeto.			

Identificación y Autentificación

La identificación y la autentificación es un requerimiento de un sistema de seguridad en todos los niveles. El libro naranja requiere que la identificación del usuario antes de ejecutar cualquier tarea que requiera interacción con el TCB (p.e. correr un programa, leer un archivo o invocar cualquier función que requiere que el sistema cheque los permisos de acceso). En la mayoría de los sistemas multiusuario, la identificación en el sistema se hace a través de algún tipo de nombre identificador (logín), seguido de un pasword.
El libro naranja establece que el password debe ser protegido, pero no dice como, existen dos publicaciones adicionales por el gobierno de los Estados Unidos que proporcionan sugerencias concretas:

- The Department of Defense Password Management Guideline (El Libro Verde)
- FIPS PUB 112 - Password Usage,

El libro verde defiende tres características principales

1. Los usuarios deben ser capaces de cambiar sus passwords
2. Los passwords deben ser generados por la maquina más el creado por el usuario
3. Seguridad en reportes de auditoria (fecha y hora del último login) debe ser proporcionado por el sistema directamente al usuario.

C1	C2	B1	B2	B3	A1
Identificación y autentificación					
El TCB debe solicitar la identificación de los usuarios antes de empezar a ejecutar cualquier acción que el TCB deba de ejecutar. El TCB debe usar algún mecanismo de protección (passwords) para autentificar la identidad del usuario. El TCB debe proteger los datos de autentificación de manera que no puedan ser accesados por usuarios no autorizados	Requerimientos adicionales El TCB debe ser capaz de reforzar las cuentas individuales al proporcionar la capacidad de identificación única a cada usuario individual ADP. El TCB debe también proporcionar la capacidad de asociar la identidad con toda acción audible elegida por esa persona.	Requerimientos adicionales El TCB debe mantener los datos de autentificación que incluyen la información para verificar la identidad de los usuarios (password) Así como la información para detectar la autorización de usuarios individuales. Los datos deben ser usados por el TCB para autentificar la identidad de los usuarios y asegurar que el nivel de seguridad y la autorización de todos los usuarios externos al TCB puedan ser creados para actuar en nombre del usuario individual que se documenta por el pase y la autorización del tipo de usuario	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales

Rutas Seguras

Una ruta segura proporciona un medio libre de errores, por el cual un usuario (típicamente una terminal o un a estación de trabajo) puede comunicarse directamente con un TCB sin interactuar con el sistema a través de aplicaciones inseguras (y posiblemente poco fiables) y capas del sistema operativo. Una ruta segura es un requerimiento para sistemas clasificados como B2 en adelante.

C1	C2	B1	B2	B3	A1
Rutas seguras					
No se requiere	No se requiere	No se requiere	El TCB debe soportar una ruta segura de comunicaciones entre él y un usuario para su identificación y autentificación. La comunicación vía esta ruta deberá ser iniciada exclusivamente por el usuario	Requerimientos adicionales El TCB debe soportar una ruta segura de comunicaciones entre él y usuarios para usarse cuando una conexión TCB a usuario es requerida (login, cambiar algún nivel de seguridad). Las comunicaciones vía ruta segura deben ser activadas exclusivamente por el usuario o el TCB y deben ser aisladas y libres de errores así como distinguibles de otras conexiones	No se tienen requerimientos adicionales

Auditoría

La auditoría es el registro, examen y revisión de las actividades relacionadas con la seguridad en un sistema confiable. Una actividad relacionada con la seguridad es cualquier acción relacionada con el acceso de usuarios, o acceso a objetos. En términos de auditoria, algunas actividades son llamadas frecuentemente eventos, y una auditoria interna se llama algunas veces eventos logging.

Eventos Típicos

Los eventos típicos incluyen

- Logins (exitosos o fallidos)
- Logouts
- Accesos a sistemas remotos
- Operaciones de archivos, apertura, renombrar, eliminación.
- Cambios en los privilegios y atributos de seguridad (cambiar en un archivo la etiqueta sensitiva o el nivel del pase de un usuario)

¿Porque auditar estos eventos? La principal razón es que hasta el sistema más seguro es vulnerable a ser atacado, y la auditoría proporciona un excelente medio de determinar cuando y como un ataque puede ser efectuado.

La auditoría permite funciones muy útiles de seguridad: Inspección y reconstrucción. La supervisión es el monitoreo de la actividad del usuario. Este tipo de auditoría, puede prevenir de que violaciones de seguridad puedan ocurrir, esto solo porque los usuarios saben que alguien los esta observando. La reconstrucción es la habilidad de poner junto, al evento de violación de seguridad, un registro de que sucedió, que necesita ser arreglado y quien es el responsable.

Cada vez que un evento auditable ocurre, el sistema escribe al final la siguiente información (Ordenada por el Libro Naranja)

- Fecha y hora de cada evento
- Identificado ID único del usuario que ejecuto el evento
- Tipo de evento
- Si el evento fue exitoso o no
- Origen de la petición (identificador de la terminal)
- Nombre de los objetos involucrados (nombre de (ej. Nombre de los archivos a ser borrados)
- Descripción y modificación a las bases de datos de seguridad
- Niveles de seguridad de los usuarios y objetos (B1 en adelante)

La auditoria es una herramienta vital de administración. Al observar patrones o actividad sospechosa (p.e. un gran número de login fallados desde una terminal en particular o los repetitivos intentos de un usuario de leer archivos a los que él no tiene acceso).
Algunos proveedores proporcionan utilerias que permiten llevar la auditoria y realizar pistas para ser impresas para usuarios particulares, para tipos específicos de eventos o para archivos particulares. Los eventos típicos incluyen eventos del sistema, eventos de archivos, y eventos de usuarios.

C1	C2	B1	B2	B3	A1
Auditoría					
No se requiere	El TCB debe ser capaz de crear, mantener y proteger de modificaciones, o acceso de usuarios no autorizados o destrucción de pistas de auditoria o accesos a objetos protegidos. La auditoría de datos debe ser protegida por el TCB de accesos de lectura o limitar a quien esta autorizado para auditar los datos. El TCB debe ser capaz de registrar los siguientes tipos de eventos: Uso de mecanismos de identificación y autentificación, introducción de objetos en el espacio direccionable del usuario (apertura de archivos, inicialización de programas), eliminación de objetos, acciones tomadas por operadores de la computadora y administradores del sistema	Requerimientos adicionales El TCB también debe ser capaz de auditar cualquier sustitución de marcas de salida legibles al humano Para eventos que introducen un objeto dentro del espacio direccionable del usuario y para borrar eventos de objetos el registro de auditoria debe incluir el nombre de los objetos y el nivel de seguridad del objeto. El administrador de sistema ADP debe ser capaz de auditar selectivamente las acciones de algún o varios usuarios basándose en la identidad individual y/o nivel de seguridad de los objetos.	Requerimientos adicionales El TCB debe ser capaz de auditar los eventos identificados que pueden ser usados en la explotación o cubierta de canales de almacenamiento	Requerimientos adicionales El TCB debe contar con un mecanismo con la capacidad de monitorear las ocurrencias o acumulación de eventos de seguridad auditable que pueden indicar de una inminente violación a las políticas de seguridad. Este mecanismo deberá de ser capaz de notificar inmediatamente al administrador de seguridad cuando se excede el umbral, y si la acumulación de ocurrencias de eventos relevantes de seguridad continua, el sistema deberá tomar la última acción disolvente que termine con este evento	No se tienen requerimientos adicionales

C1	C2	B1	B2	B3	A1
Auditoría					
	y/o administradores de la seguridad del sistema, y otros eventos relevantes del sistema. Para cada evento registrado, el registro de auditoria deberá identificar: fecha y hora del evento, y si el evento fue exitoso o fallo el evento. La identificación / autentificación de eventos que originan la petición (ID de la terminal) deberán ser incluidos en el registro de auditoria El administrador de sistema ADP, debe ser capaz de seleccionar las acciones a auditar de uno o de varios usuarios basándose en la identidad individual				

Arquitectura del Sistema

El requerimiento de arquitectura del sistema tiene el objeto de diseñar un sistema para hacerlo lo más seguro posible, - sino invulnerable.
Así los sistemas de los niveles bajos (C1, B1 y hasta B2) no fueron necesariamente diseñados específicamente para seguridad, ellos soportan principios de diseño de hardware y sistema operativo, tan bien como la habilidad de soportar características específicas que quizás son agregadas a estos sistemas. La mayoría de los diseños modernos de multiprocesamiento, y sistemas multi usuarios siguen las claves los principios de diseño necesarios para cumplir los requerimientos del libro naranja en los que arquitectura del sistema se refiere al menos C2 y B1, sí bien estos principios no están necesariamente orientados a seguridad

C1	C2	B1	B2	B3	A1
Arquitectura del sistema					
EL TCB debe mantener un dominio para su propia ejecución que lo proteja de interferencia externa o falsificaciones (Ej. Para modificación de su código o estructura de datos).	Requerimientos adicionales: El TCB debe aislar los recursos a ser protegidos de manera que los usuarios tengan control de acceso y requerimientos de auditoría	Requerimientos adicionales El TCB debe mantener procesos aislados así como proporcionar distintas direcciones de espacio bajo su control	Nuevos Requerimientos para B2 El TCB debe mantener un dominio para su propia ejecución de protecciones de interferencia externa o falsificaciones(Ej. Para modificación de su código o estructura de datos).	Requerimientos adicionales El TCB debe diseñar y estructurar el uso completo, de un mecanismo de protección, conceptualmente simple con definición semántica precisa. Este mecanismo debe jugar un papel central en el reforzamiento de la estructura interna entre el TCB y el sistema.	No se tienen requerimientos adicionales

C1	C2	B1	B2	B3	A1
Arquitectura del sistema					
Los recursos controlados por el TCB pueden ser definidos en un subgrupo así como los usuarios y objetos en el sistema ADP.			El TCB debe mantener procesos aislados así como proporcionar dirección de espacios distintas bajo su control. El TCB debe estar estructurado internamente dentro de una bien definido módulo independiente. El módulo TCB debe ser diseñado bajo el principio de que los privilegios sean reforzados, Características de hardware, así como segmentación, debe ser usado para soportar lógicamente distinciones de objetos almacenados con atributos separados (nombrar, leer y escribir). La interfaz de usuario del TCB debe ser completamente definida y todos los elementos del TCB identificados	El TCB debe incorporar el uso significativo de capas, abstracción y ocultamiento de datos. Una aplicación de ingeniería de sistemas significativa debe ser directamente conducida minimizando la complejidad del TCB y excluyendo de los módulos del TCB los objetos que no presentan protección crítica	No se tienen requerimientos adicionales

Integridad del Sistema

La integridad del sistema significa que el hardware y el firmware debe trabajar y debe ser probado para asegurar que trabaje adecuadamente, Para todos los niveles, el libro naranja establece “las características de hardware y software que deben ser proporcionadas para ser usadas y periódicamente validadas para la correcta operación del hardware instalado y los elementos firmware del TCB

La integridad de sistema una meta de vital importancia para todos los desarrolladores de sistemas, y no solo desarrolladores de sistemas seguros. Como ya se ha mencionado anteriormente, un elemento muy importante de un sistema de seguridad es la habilidad de que el sistema funcione como se espera y permanecer en operación

Muchos vendedores miden los requerimientos de integridad del sistema, al proveer de un juego de pruebas de integridad, EL más substancial diagnostico es hacer un programa calendarizado de periodos de mantenimiento preventivo.

C1	C2	B1	B2	B3	A1
Integridad del sistema					
Las características del hardware y/o el software deben ser proporcionadas para ser usadas y periódicamente validadas su correcta operación así como los elementos de hardware y firmware del TCB	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales

Análisis de Canales Secretos

Un canal secreto es una ruta de información que no se usa ordinariamente para comunicaciones en un sistema, por los mecanismos normales de seguridad del sistema. Es una vía secreta para transportar información a otra persona o programa – El equivalente computacional de un espía que porta un periódico como una contraseña.
En teoría cada pieza de información almacenada o procesada por un sistema computacional seguro es un potencial canal secreto.
Existen dos tipos de canales secretos, canales de almacenamiento y canales de temporización. Los canales de almacenamiento transportan información para cambiar datos almacenados en el sistema en alguna forma. Los canales de temporización transportan información que afecte el desempeño o modifiquen de alguna forma el tiempo usado por los recursos del sistema en alguna forma medible.

C1	C2	B1	B2	B3	A1
Análisis de canales secretos					
No se requiere	No se requiere	No se requiere	El sistema desarrollado deberá comportarse completamente, buscando la simulación de canales de almacenamiento y haciendo determinaciones (para las mediciones actuales o por estimaciones de ingeniería) o el máximo ancho de banda de cada canal identificado	Requerimientos adicionales: Búsqueda de todos los canales simulados (almacenamiento y temporización)	Requerimientos adicionales: Métodos formales deben de ser usados en el análisis

Administración de Seguridad

La facilidad de la administración de seguridad es la asignación de un individuo específico para administrar las funciones relacionadas con la seguridad de un sistema. La facilidad de administración de la seguridad es muy relacionada con el concepto de *privilegio mínimo,* un concepto tempranamente introducido en términos de arquitectura de sistemas. En el contexto de seguridad, el privilegio mínimo significa que el usuario de un sistema debe tener el menor número de permisos y la menor cantidad de tiempo – únicamente el necesario para desempeñar su trabajo. También esta relacionado el concepto de administración con la separación de obligaciones, la idea es que es mejor asignar piezas de seguridad relacionadas con tareas de algunas personas específicas y que ningún usuario tenga el control total de los mecanismos de seguridad del sistema, para que de ninguna forma un usuario pueda comprometer completamente al sistema

C1	C2	B1	B2	B3	A1
Facilidad de administración de la seguridad					
No se requiere	No se requiere	No se requiere	El TCB debe soportar separadamente las funciones de administrador y operador	Requerimientos adicionales Las funciones ejecutadas en el papel del administrador de seguridad deben ser identificadas. El Personal de Administración del sistema ADP, deberá solo ser capaz de ejecutar funciones de administrador de seguridad	No se tienen requerimientos adicionales

C1	C2	B1	B2	B3	A1
Facilidad de administración de la seguridad					
No se requiere	No se requiere	No se requiere	El TCB debe soportar separadamente las funciones de administrador y operador	después de tomar una acción auditable distinguible al asumir el papel de administrador de la seguridad en el sistema ADP. Las funciones que no son de seguridad que pueden ser ejecutadas por el papel de administrador de seguridad deberán limitarse estrictamente a lo más esencial para ejecutar la seguridad efectivamente	No se tienen requerimientos adicionales

Recuperación Confiable

La recuperación confiable asegura que la seguridad no ha sido violada cuando se cae un sistema o cuando cualquier otra falla del sistema ocurre
La recuperación confiable actualmente involucra dos actividades: prepararse ante una falla del sistema y recuperar el sistema.
La principal responsabilidad en preparación es respaldar todos los archivos del sistema crítico con una base regular. El procedimiento de recuperación puede ser con mucho, esforzarse por restaurar solo un día o dos de procesamiento de información.

Si una falla inesperada ocurre, como una falla de disco duro, o un corte de corriente eléctrica, se debe recuperar el sistema de acuerdo con ciertos procedimientos para asegurar la continuidad de la seguridad en el sistema. Este procedimiento también puede ser requerido si se detecta un problema del sistema, como recursos perdidos, o una base de datos inconsistente o cualquier cosa que comprometa el sistema

C1	C2	B1	B2	B3	A1
Recuperación confiable					
No se requiere	No se requiere	No se requiere	No se requiere	Los procedimientos y/o mecanismos deberán ser proporcionados para asegurar que, después de una falla del sistema ADP u otra discontinuidad, el sistema se recupere sin un obtener compromiso de protección	No se tienen requerimientos adicionales

Diseño de Especificaciones y Verificación

El diseño de especificaciones y la verificación requiere una comprobación de que la descripción del diseño para el sistema sea consistente con las políticas de seguridad del sistema.
A cada nivel de seguridad empezando desde el B1, el libro naranja. Requiere un incremento del modelo formal (precisamente matemático) de las políticas del sistema de seguridad que permite se incrementen las pruebas de que el diseño del sistema es consistente con su modelo

¿Qué es una prueba formal? Es un argumento matemático completo y convincente de que el sistema es seguro, o al menos de que el diseño del sistema y lleva implementada una adecuada política de seguridad. Por ejemplo, si se demuestra matemáticamente que bajo condiciones existen ciertos sujetos (usuarios), que pueden accesar a cierto tipo de objetos (archivos) y se demuestra que los usuarios no pueden engañar las condiciones de acceso.

C1	C2	B1	B2	B3	A1
Diseño de especificaciones y verificación					
No se requiere	No se requiere	Un modelo formal o informal de las políticas de seguridad soportadas por el TCB que deberá ser mantenido durante todo el ciclo de vida del sistema ADP y demostración de ser consistente con su axioma	Requerimientos adicionales para B2 Un modelo formal de la política de seguridad soportada por el TCB deberá ser mantenida durante todo el ciclo de vida del sistema ADP que deberá proporcionar consistencia con su axioma. Especificación descriptiva de alto nivel (DTLS) del TCB en términos de excepciones, mensajes de error y efectos. Este deberá ser mostrado de ser una descripción exacta de la interfaz del TCB	Requerimientos adicionales Un argumento convincente deberá ser proporcionado de que el DTLS es consistente con el modelo	Requerimientos adicionales Una especificación formal de alto nivel (FTLS) del TCB que deberá ser mantenido y precisamente descrito el TCB en términos de excepciones, mensajes de error y efectos. EL DTLS y el FTLS deberá incluir los componentes del TCB que están implementados como hardware y/o firmware si sus propiedades son visibles para él la interfaz del TCB. Una combinación de técnicas formales e informales deberá ser usada para mostrar que el FTLS es consistente con el modelo.

Pruebas de Seguridad

El libro naranja tiene un substancial interés en probar las características de seguridad en los sistemas a evaluar. Las pruebas de seguridad aseguran que los requerimientos están relacionados con los requerimientos de pruebas de documentación. El sistema desarrollado será probado para todas las características de seguridad, asegurando que el sistema trabaja como se describe en la documentación, y se documenten los resultados de las pruebas de estas características. El equipo de evaluación del NTSC esta comprometido con sus pruebas.

Estos son los dos tipos básicos de pruebas de seguridad:

- Prueba de mecanismos y
- Prueba de interfaz.

La prueba de mecanismos significa probar los mecanismos de seguridad, estos mecanismos incluye control de acceso discrecional, etiquetado, control de acceso obligatorio, Identificación y autentificación, prueba de rutas, y auditoría.
La prueba de interfaz significa el probar todas las rutinas del usuario que involucren funciones de seguridad

C1	C2	B1	B2	B3	A1
Pruebas de seguridad					
Los mecanismos de seguridad del sistema ADP deberá ser probado y encontrado trabajando y exigido en la documentación del sistema. Las pruebas deberán ser hechas para asegurar que no hay caminos obvios para acceso de usuarios no autorizados o cualquier otra falla en el mecanismo de protección de la seguridad del TCB	Requerimientos adicionales Las pruebas deberán también ser incluidas en la búsqueda de banderas obvias que puedan permitir una violación de recursos aislados, o que puedan permitir el acceso no autorizado de auditoría o autentificación de datos	Requerimientos adicionales para B1 Los mecanismos de seguridad del sistema ADP deberán ser probados y encontrados trabajando con la documentación del sistema. Un equipo de individuos que entiendan completamente la implementación específica del TCB deberá diseñar documentación, código fuente y código objeto para el análisis completo y Las pruebas. Estos objetivos deberán descubrir todo el diseño y la implementación de banderas que pudieran permitir a un sujeto externo al TCB el leer, cambiar o borrare datos normalmente denegados bajo políticas de seguridad discrecional u	Requerimientos adicionales El TCB deberá ser encontrado relativamente resistente a penetración Al probar todo deberá demostrarse que la implementación del TCB es consistente con la descripción de especificación de alto nivel.	Requerimientos adicionales El TCB deberá ser encontrado resistente a penetraciones, Ninguna bandera de diseño y ninguna bandera de implementación sin correcciones debe ser encontrada durante las pruebas y deberán ser razonablemente confidenciales las pocas que queden.	Requerimientos adicionales Las pruebas deberán demostrar que la implementación del TCB es consistente con la especificación formal de alto nivel El manual u otros mapas del FTLS del código fuente pueden formar bases para las pruebas de penetración.

C1	C2	B1	B2	B3	A1
Pruebas de seguridad					
		obligatorias reforzadas por el TCB, así como el asegurar que ningún sujeto (sin autorización para hacerlo) sea capaz de causar que el TCB entre en un estado tal que sea incapaz de responder a comunicaciones iniciadas por otros usuarios. Todas las banderas descubiertas deberán ser removidas o neutralizadas y el TCB vuelto a probar para demostrar que estas han sido eliminadas y que nuevas banderas no han sido introducidas			

Administración de Configuración

La administración de configuraciones protege un sistema seguro mientras esta siendo diseñado, desarrollado, y mantenido. Involucra el identificar, controlar, contabilizar y auditar todos los cambios hechos en los lineamientos de TCB, incluyendo hardware, firmware y software, por ejemplo, cualquier cambio en el código, durante las faces de diseño, desarrollo y mantenimiento así como la documentación, planes de pruebas, y otras herramientas del sistema relacionadas y sus facilidades.
La administración de configuraciones tiene varias metas, primero, el control del mantenimiento del sistema durante su ciclo de vida, asegurando que el sistema es usado de la forma correcta, implementando las políticas de seguridad adecuadas. El "sistema adecuado" es el sistema que ha sido evaluado o que actualmente esta siendo evaluado En otras palabras la administración de configuraciones previene de usar versiones obsoletas 8º nuevas, que no han sido probadas en el sistema) o alguno de sus componentes.

Segundo, hace posible el regresar a versiones previas del sistema. Esto es importante, si por ejemplo, un problema de seguridad es encontrado en una versión del sistema que no tenían en una versión anterior.
Para cumplir los requerimientos de la administración de configuración se necesita:

- Asignar un identificador único para cada elemento configurable
- Desarrollar un plan de administración de la configuración
- Registrar todos los cambios de elementos de configuración (en línea y fuera de línea)
- Establecer un tablero de control e configuraciones

C1	C2	B1	B2	B3	A1
Administración de configuración					
No se requiere	No se requiere	No se requiere	Durante el desarrollo y mantenimiento del TCB, una administración de configuraciones deberá tomar lugar en el control de mantenimiento de los cambios en la especificación descriptiva de alto nivel y otros datos de diseño, documentación de implementación, código fuente, las versiones corridas del código objeto y las pruebas de correcciones y documentación.	No se tienen requerimientos adicionales	Nuevos Requerimientos para A1 Durante el ciclo completo de vida... durante el diseño, desarrollo, y mantenimiento del TCB, una administración de configuraciones deberá tener lugar para todos el hardware, firmware y software relacionado con la seguridad y debe de mantenerse un control formal de mantenimiento de todos los cambios al

C1	C2	B1	B2	B3	A1
Administración de configuración					
			La administración de configuraciones del sistema deberá asegurar un mapeo consistente entre toda la documentación y el código asociado con las versiones actuales del TCB. Las herramientas deberán tenerse para generar una nueva versión del TCB desde el código fuente. También deberán estar disponibles las herramientas para hacer comparaciones de la nueva versión generada, con la versión previa del TCB en orden a determinar que sólo los cambios proyectados han sido hechos en el código que actualmente se esta usando como la nueva versión del TCB		modelo formal las especificaciones descriptiva y formal de alto nivel, otros datos de diseño, documentación e implementación, código fuente, la versión actual del código objeto, las pruebas de reparaciones y la documentación. La administración de configuraciones del sistema deberá asegurar un mapeo consistente entre toda la documentación y el código asociado con las versiones actuales del TCB. Las herramientas deberán tenerse para generar una nueva versión del TCB desde el código fuente. También las herramientas deberán ser mantenidas bajo un estricto control de configuraciones para comparar una versión nueva generada desde el TCB en orden a determinar que sólo los cambios proyectados han sido hechos en el código que actualmente se esta usando.

Distribución Confiable

La distribución confiable protege un sistema seguro mientras el sistema es siendo transportado al sitio del cliente. Este requerimiento solo se tiene para el nivel A1, este requerimiento tiene dos metas protección y validación del lugar
La protección significa que el vendedor final (y durante el transporte del vendedor al cliente), se asegura que durante la distribución, el sistema llegue al lugar donde lo solicito el cliente, exactamente, como fue evaluado antes de transportarse por el vendedor, ya que proporciona protección durante el empaque, transporte entre intermediarios hasta llegar al usuario final.
Validación del lugar, significa que el cliente final, con la distribución confiable puede detectar falsificaciones del sistema o modificación del sistema.

C1	C2	B1	B2	B3	A1
Distribución Confiable					
No se requiere	No se requiere	No se requiere	No se requiere	No se requiere	Un sistema de control ADP confiable y facilidad de distribución deberá ser proporcionada para mantener la integridad del mapeo entre los datos maestros que describen la versión actual del TCB y la copia maestra en sitio del código del la versión actual. Los procedimientos (Prueba de aceptación de la seguridad del sitio) deberá existir para asegurar que el software, firmware y actualización del hardware del TCB, distribuido a los clientes es exactamente como se especifica en las copias principales.

Guía del Usuario de Características de Seguridad

La guía del usuario de características de seguridad (SFUG) es un apunte ordinario, sin privilegios para todos los usuarios del sistema. En el se encuentran cosas que es necesario saber acerca de las características del sistema de seguridad y de cómo es que están reforzadas. Los temas típicos incluyen:

- Acceso al sistema seguro. Como se debe introducir el login y el password, con que frecuencia debe de cambiarse, que mensajes deben de verse, cómo deben de usarse estos mensajes para reforzar la seguridad del sistema
- Protección de archivos y otro tipo de información. Cómo se debe de especificar una lista de control de acceso (o protecciones similares)
- Importar y exportar archivos Como leer nuevos datos dentro del sistema confiable y como escribir datos de otros sistemas sin arriesgar la seguridad

C1	C2	B1	B2	B3	A1
Guía del usuario de características de seguridad					
Un resumen sencillo, capítulo o manual en la documentación del usuario que describa los mecanismos de protección proporcionados por el TCB, lineamientos sobre su uso y como interactuar con otros.	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales

Facilidades del Manual de Seguridad

Este documento es un apunte de administrador del sistema y/o administradores de seguridad. Habla sobre todas las cosas que se necesita saber acerca de la configuración del sistema para ser seguro, reforzando el sistema de seguridad, interactuando con peticiones del usuario y haciendo que el sistema trabaje con las mejores ventajas. EL Libro naranja requiere que este documento contenga advertencias, acerca de las funciones y privilegios que deben ser controlados en sistemas seguros

C1	C2	B1	B2	B3	A1
Facilidades del manual de seguridad					
Un direccionamiento manual por parte del administrador del sistema ADP deberá presentar avisos sobre sus funciones y privilegios que deberá de controlar cuando ejecuta una instalación segura	Requerimientos adicionales Los procedimientos para examinar y mantener los archivos de auditoría así como las estructuras de los registros detallados de auditoría para cada tipo de evento auditable debe ser proporcionado	Requerimientos adicionales EL manual deberá describir las funciones del operador y del administrador relativas a la seguridad, al incluir los cambios de las características de seguridad para los usuarios.	Requerimientos adicionales Los módulos del TCBN que contienen los mecanismos de validación de referencias deberán ser identificables. Los procedimientos para una operación segura de un nuevo TCB desde origen, después de modificarse por cualquier módulo en el TCB deberá ser descrito	Requerimientos adicionales Se deberán incluir los procedimientos para asegurar que el sistema es inicialmente arrancado de una modo seguro, Los procedimientos deberán también estar incluidos en el compendio de operación del sistema de seguridad después de cualquier lapso de operación del sistema	No se tienen requerimientos adicionales

C1	C2	B1	B2	B3	A1
Facilidades del manual de seguridad					
		Este deberá proporcionar lineamientos para el uso consistente y efectivo de las características de protección del sistema, como deberá interactuar, como generar una nueva TCB segura y los procedimientos de instalación, advertencias, y privilegios que deberán ser controlados para operar las instalaciones de una manera segura			

Documentación de Pruebas

Para el libro naranja, consiste en mostrar como los mecanismos de seguridad fueron probados, y los resultados de los mecanismos de seguridad con pruebas funcionales
El tener buena documentación de pruebas es generalmente sencillo pero voluminoso. Es común que la documentación de pruebas para los sistemas C1 y C2 consista en varios volúmenes de descripción de pruebas y resultados

C1	C2	B1	B2	B3	A1
Documentación de pruebas					
El desarrollador del sistema deberá proporcionar a los evaluadores un documento que describa el plan de pruebas, procedimientos de prueba que muestren como los mecanismos son probados, y los resultados de las pruebas funcionales de los mecanismos de seguridad	No se tienen requerimientos adicionales	No se tienen requerimientos adicionales	**Requerimientos adicionales** Se deberá incluir los resultados de las pruebas de falta de efectividad de los métodos usados para reducir los anchos de banda de los canales secretos	No se tienen requerimientos adicionales	**Requerimientos adicionales** Los resultados del mapeo ente las especificaciones formales de alto nivel y el código fuente del TCB deberán ser proporcionadas

Diseño de Documentación

Es un requerimiento formidable para todos los desarrolladores de sistemas. La idea de diseñar documentación es documentar internamente el sistema (o lo más básico del TCB) hardware, firmware y software. El objetivo del diseño de documentación es que "la filosofía del fabricante sobre protección y... cómo esta filosofía es trasladada dentro del TCB" Una tarea clave que define los límites del sistema y distingue claramente entre cuales porciones del sistema son relevantemente seguras y cuales no.

Las dos mayores metas del diseño de documentación son: el probar al equipo de evaluación que el sistema cumple con el criterio de evaluación y el auxiliar al equipo de diseño y desarrollo para ayudar a definir las políticas del sistema de seguridad y como hacer que las políticas se lleven a cabo durante la implementación.

C1	C2	B1	B2	B3	A1
Diseño de documentación					
La documentación que proporcione una descripción de la filosofía del fabricante sobre protección deberá estar disponible, y una explicación de cómo esta filosofía es trasladada dentro,	No se tienen requerimientos adicionales	Requerimientos adicionales Una descripción formal o informal del modelo de las políticas de seguridad reforzado por el TCB deberá estar disponible para dar una explicación de que es suficiente el reforzar las políticas de seguridad.	Requerimientos adicionales Las interfaces entre los módulos del TCB deberán ser descritos El modelos de políticas de seguridad deberá ser formal y probado. La especificación descriptiva de alto nivel (DTLS) deberá ser mostrada en una descripción exacta de la interfaz del TCB. .	Requerimientos adicionales La implementación del TCB (hardware, firmware y software) deberá ser informalmente mostrada y ser consistente con el DTLS. Los elementos del DTLS deberán ser mostrados, usando técnicas	Requerimientos adicionales La implementación del TCB deberá ser informalmente mostrada para ser consistente con la especificación formal de alto nivel (FTLS). Los elementos del FTLS deberán ser mostrados, usando técnicas

C1	C2	B1	B2	B3	A1
Diseño de documentación					
del TCB, sí el TCB es compuesto por distintos módulos las interfaces entre estos módulos deberá ser descrita.		El mecanismo de protección específica del TCB deberá ser identificable y una explicación que demuestre cómo éste mecanismo satisface el modelo.	La documentación describirá como el TCB implementa el concepto de monitor de referencia y dar una explicación de porque es resistente a penetración, y no puede ser traspasado, y es correctamente implementado. La documentación deberá describir como el TCB se estructura para pruebas de instalación y reforzar los menores privilegios. Esta documentación deberá también presentar los resultados del análisis de los canales secretos y los intercambios involucrados al restringir los canales. Todos los eventos auditables que pueden ser usados en la explotación de conocer canales de almacenaje secretos, deberán ser identificados	de información, con su correspondiente elemento del TCB	de información, con su correspondiente elemento del TCB Los mecanismos de hardware, firmware y software no compartidos con el FTLS pero estrictamente internos del TCB (mapeo de registros, acceso directo a memoria de entrada/salida), deberá ser claramente descrito.

Glosario de Términos

ADP.	Automatic Data Processing (Procesamiento automático de datos).
Aplicaciones sensitivas.	Son todos aquellos programas y sistemas desarrollados para la administración de sistemas, como pueden ser herramientas administración, configuración o seguridad.
DOD	Departament of Defense (Departamento de Defensa de los Estados Unidos).
Información sensitiva	Es toda aquella información que no esta disponible a todos los usuarios por poseer un cierto grado de confidencialidad.
Elemento Activo	Son todos aquellos usuarios o procesos que poseen la capacidad de crear, modificar, leer, escribir o borrar información
Etiqueta	Son identificadores que se les asignan a los usuarios o a los objetos dentro del sistema, se utilizan estos identificadores para verificar los permisos que tiene el usuario o el objeto para permitir o denegar las acciones.
Etiqueta Sensitiva de Usuario	Específica el grado, o nivel de confianza, asociado con ese usuario, las etiquetas de usuario sensitivas es usualmente llamada como certificado de paso ó "clearance".
Etiqueta Sensitiva de Archivo	Especifica el nivel de confianza que un usuario puede ser capaz de tener al tener acceso a ese archivo.
Evento	Son todas las acciones generadas por un usuario o un proceso que van a exigir una respuesta por parte de un objeto.
Firmware	Se define como hardware en software, es decir memorias ROM que contienen instrucciones o datos necesarios para el sistema, un ejemplo son los BIOS de la mayoria de las computadoras.

Nivel de Sensitividad	Es cuando toda la información almacenada o todos los usuarios que tienen acceso a esa información poseen exactamente los mismos permisos.
Objeto	Son todos los elementos identificables dentro del sistema, cmomo son directorios, archivos, dispositivos, puertos, etc.
TCB	Trusted Computers Bases (Computadora Confiable Base).

Bibliografía

URL: http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

Computer Security Basics,
Deborah Russell and G.T. Gangemi Sr.
O'Reilly & Associates, Inc.